**Вопросы к зачету**

1. Основные определения, связанные с защитой ОС. Адекватная политика безопасности ОС.
2. Основные подходы к созданию защищенных ОС.
3. Общие представления об идентификации и аутентификации.
4. Общие представления об авторизации и разграничении прав доступа к объектам ОС.
5. Мандатное управление доступом.
6. Дискреционное управление доступом.
7. Изолированная программная среда.
8. Общие представления об аудите системы защиты и сканере безопасности.
9. Классификация угроз безопасности.
10. Атаки на безопасность ОС.
11. Управление доступом. Основные определения.
12. Права доступа в UNIX.
13. Разделяемые каталоги. Подмена идентификатора процесса.
14. Дополнительные биты доступа. Права доступа по умолчанию. Суперпользователь.
15. Ограничения базовой модели управления доступом в UNIX. Дополнительные права доступа.
16. Ограничения базовой модели управления доступом в UNIX. POSIX ACL.
17. Ограничения базовой модели управления доступом в UNIX. POSIX capabilities.
18. Управление доступом в Windows. Объекты и субъекты доступа.
19. Идентификатор безопасности SID. Структура идентификатора безопасности.
20. Методы и права доступа в Windows. Привилегии субъектов доступа.
21. Маркер доступа. Механизм олицетворения.
22. Дескриптор защиты объекта (дескриптор безопасности).
23. Проверка прав доступа субъекта к объекту.
24. Уровни целостности. Назначение дескрипторов защиты создаваемым объектам.
25. Мандатный контроль целостности (MIC & UAC).
26. Элементы изолированной среды (интерфейс SAFER).
27. Парольная аутентификация.
28. Аутентификация с использованием внешних носителей.
29. Биометрическая аутентификация.
30. Аутентификация в UNIX. Классический подход.
31. Аутентификация в UNIX. PAM модули.
32. Локальная аутентификация в Windows.
33. Аутентификация при удаленном входе в Windows.
34. Аудит. Общие сведения.
35. Системы обнаружения вторжений.
36. Аудит в Windows. Журнал аудита. Категории событий.
37. Аудит в Windows. Политика аудита и атрибуты защиты.
38. Аудит в Windows. События и задачи. Подписка на события аудита.
39. Аудит в UNIX. syslogd, klogd.
40. Аудит в UNIX. auditd.
41. Домены в Windows. Общие сведения.
42. Сквозная аутентификация.
43. Отношения доверия.
44. Активный каталог.
45. Групповая политика.

**Литература**

1. Проскурин В.Г. Защита в операционных системах. – М:, Горячая линия – Телеком, 2014.
2. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. – М.: Машиностроение, 2007.
3. Хорев П.Б. Программно-аппаратная защита информации. – М.: Форум, 2012.
4. Таненбаум Э., Х. Бос Современные операционные системы. - СПб.: Питер, 2015.
5. Столлингс В. Опрерационные системы. - М.: Вильямс, 2002.
6. Робачевский А.М., Немнюгин С.А., Стесик О.Л. Операционная система UNIX. – СПб.: БХВ – Петербург, 2008.

**Примерные темы рефератов**

1. Выявленные уязвимости современных операционных систем.
2. Биометрическая аутентификация пользователя.
3. Аутентификация с использованием внешних носителей.
4. Современные парольные взломщики.
5. Взлом парольной защиты в операционных системах.
6. Программные закладки (внедрение, выявление и защита от них).
7. Настройка аудита в операционных системах UNIX.
8. Настройка аудита в операционных системахWindows.
9. Системы обнаружения вторжений.
10. Механизмы защиты службы каталогов Actve Directory.
11. Сквозная аутентификация.
12. Управление доступом на основе ролей (Role-based Access Control, RBAC).
13. Модель доступа тип-домен (Domain Type Enforcement, DTE).
14. Модель безопасности Белла-Ла Падулы.
15. Защита в мобильных операционных системах.
16. Протокол сетевой аутентификации Kerberos.
17. POSIX ACL.
18. POSIX capabilities.
19. Интерфейс SAFER.
20. PAM модули UNIX.

**Требования к оформлению реферата**

Объем реферата – 10 – 15 стр. печатного текста. Шрифт – не более 14 pt, TimesNewRoman, интервал – 1,5, поля: верхнее, нижнее, левое – 2 см, правое 1,5 см.

На титульном листе указывается название работы, ФИО студента и группа, ФИО преподавателя (научного руководителя), проверяющего и оценивающего реферат, наименование кафедры и учебного заведения. ***Тема реферата выбирается по согласованию с преподавателем и может быть сформулирована самостоятельно.***

Название работы оформляется следующим образом:

**Реферат по дисциплине «Защита в операционных систем» на тему: «……»**

Текст реферата печатается на одной стороне страницы; сноски и примечания печатаются на той же странице, к которой они относятся (через 1 интервал, более мелким шрифтом, чем текст). Основной текст должен сопровождаться иллюстративным материалом (рисунки, фотографии, диаграммы, схемы, таблицы, программы). Если в основной части содержатся цитаты или ссылки на высказывания, необходимо указать номер источника по списку, приведенному в конце реферата, и страницу в квадратных скобках в конце цитаты или ссылки.

Реферат – это краткое изложение в письменной форме содержания прочитанных книг и документов; сообщение об итогах изучения научного вопроса; доклад на определенную тему, освещающий ее вопросы на основе литературных и других источников. Целью написания реферата является углубление знаний по конкретной проблеме, получение навыков работы с научной и научно-популярной литературой.

В процессе работы над проблемой необходимо:

* вычленить проблему;
* самостоятельно изучить проблему на основе первоисточников;
* дать обзор использованной литературы;
* последовательно и доказательно изложить материал;
* правильно оформить ссылки на источники.

**Обязательные структурные элементы реферата:**

1. Введение, в котором описывается актуальность проблемы, определяются   цели и задача реферата; объем введения – 1 - 2 страницы.
2. Содержание.
3. Текст реферата должен содержать:

* обоснование выбранной темы;
* сравнительный анализ литературы по проблеме;
* изложение собственной точки зрения на проблему;
* выводы и предложения;
* заключение.

4. Список использованных источников должен оформляться в соответствии с ГОСТом и может содержать не только названия книг, журналов, газет, но и любые источники информации (например, сведения из сети Интернет, частные сообщения каких-либо специалистов, высказанные в личных беседах их с автором реферата).

Реферат излагается доступным научным (научно-популярным) языком в относительно сжатой форме с использованием облегченных синтаксических конструкций. Такие конструкции могут стать своеобразным планом реферативной статьи: “ В рассматриваемой статье ставится ряд вопросов …Автор подчеркивает, что … Более подробно рассмотрена проблема… Анализируются разные точки зрения … В заключение необходимо отметить, что …” и т.д.

При выставлении оценки за реферат учитываются следующие компоненты:

* содержательная часть (глубина проработки проблемы, структура работы, объем проанализированных источников и т.п.);
* оформление (соответствие стандарту, эстетика оформления, наличие иллюстративного материала и т.п.);
* защита реферата (ориентация в тексте реферата, ответы на вопросы и т.п.).

Реферат сдается в электронном виде.